

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA :

14 Cr. 68 (KBF)

- against - :

ROSS ULBRICHT, :

Defendant. :

-----X

REPLY MEMORANDUM OF LAW IN SUPPORT OF
DEFENDANT ROSS ULBRICHT'S POST-TRIAL MOTIONS

Joshua L. Dratel
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732 - 0707
jdratel@joshuadratel.com

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Joshua J. Horowitz

TABLE OF CONTENTS

| | |
|--|-----|
| Table of Contents..... | i |
| Table of Authorities..... | iii |
| Introduction. | 1 |
| STATEMENT OF FACTS. | 6 |
| ARGUMENT | |
| POINT I | |
| MR. ULBRICHT SHOULD BE GRANTED A NEW TRIAL BECAUSE THE GOVERNMENT FAILED TO PROVIDE EXCULPATORY MATERIAL AND INFORMATION IN A TIMELY MANNER, THEREBY DENYING HIM HIS FIFTH AMENDMENT RIGHT TO DUE PROCESS AND A FAIR TRIAL. | 8 |
| A. <i>There Was Not Any Need to Maintain Secrecy of the Investigation of Former SA’s Force and Bridges Prior to Trial In This Case.</i> | 8 |
| B. <i>The Government Continues to Misapprehend Its Obligation to Produce Exculpatory Material and Information to the Defense</i> | 9 |
| C. <i>The Government’s Investigations of Mark Karpeles and Anand Athavale Were Not Mere “Leads” or “Theories” or “Suspensions” or “Hunches”.....</i> | 21 |
| 1. <i>The Government’s Investigation of Mark Karpeles.....</i> | 21 |
| 2. <i>The Government’s Investigation of Anand Athavale.....</i> | 26 |
| D. <i>The Information That Was Not Disclosed Until the Force Complaint Was Unsealed. . .</i> | 30 |
| E. <i>What Remains Unknown (to the Defense, At Least) About SA Force’s and Bridges’s Misconduct In the Context of the Silk Road Investigation.</i> | 33 |
| F. <i>The Record Demonstrates That Silk Road Investigations Were Coordinated and, for Practical Purposes and for Determining Relevance to This Case, Combined.</i> | 38 |

| | | |
|----|--|----|
| G. | <i>The Information Regarding the Investigation of Former SA's Force and Bridges Would Be Relevant to This Case Regardless Whether the Investigations Were Independent.</i> | 51 |
| 1. | <i>The Government's Initial Exhibit List.</i> | 51 |
| 2. | <i>The Government's Opposition to Mr. Ulbricht's Motion for Bail.</i> | 54 |
| 3. | <i>The Importance of the First Half of 2013 Regarding the Evidence At Trial.</i> | 55 |
| 4. | <i>The Communications Between DeathFromAbove and DPR.</i> | 57 |
| | Conclusion. | 60 |

TABLE OF AUTHORITIES

CASES

| | |
|---|---------------------|
| <i>Brady v. Maryland</i> , 373 U.S. 83 (1963). | 9-11, 14-21, 24, 30 |
| <i>Cone v. Bell</i> , 556 U.S. 449 (2009). | 18 |
| <i>Giglio v. United States</i> , 405 U.S. 150 (1972). | 11, 30 |
| <i>Imbler v. Pachtman</i> , 424 U.S. 409 (1976). | 16 |
| <i>Leka v. Portuondo</i> , 257 F.3d 89 (2d Cir. 2001). | 10, 15-16 |
| <i>Poventud v. City of New York</i> , 750 F.3d 121 (2d Cir. 2014). | 16, 20 |
| <i>Strickler v. Greene</i> , 527 U.S. 263 (1999). | 20 |
| <i>United States v. Bin Laden</i> , 397 F. Supp. 2d 465 (S.D.N.Y. 2005) <i>aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in E. Africa</i> , 552 F.3d 93 (2d Cir. 2008). | 20 |
| <i>United States v. Bufalino</i> , 576 F.2d 446 (2d Cir.1978). | 20 |
| <i>United States v. Cobb</i> , 271 F. Supp. 159 (S.D.N.Y.1967). | 15 |
| <i>United States v. Coppa</i> , 267 F.3d 132 (2d Cir. 2001). | 10-11 |
| <i>United States v. Gil</i> , 297 F.3d 93 (2d Cir. 2002). | 15 |
| <i>United States v. Jackson</i> , 345 F.3d 59 (2d Cir. 2003). | 20 |
| <i>United States v. Jacobs</i> , 650 F. Supp. 2d 160 (D. Conn. 2009). | 10-11 |
| <i>United States v. Payne</i> , 63 F.3d 1200 (2d Cir.1995). | 20 |
| <i>United States v. Rittweger</i> , 524 F.3d 171 (2d Cir. 2008). | 10-11, 19 |
| <i>United States v. Rodriguez</i> , 496 F.3d 221 (2d Cir. 2007). | 9-10 |

STATUTES

| | |
|------------------------------|----------------------------|
| U.S. Const. Amend. X. | 7 |
| U.S. Const. Amend. XI. | 2 |
| 18 U.S.C. §3500..... | 9-11, 15-16, 19-21, 39, 57 |
| Rule 6(e), Fed.R.Crim.P..... | 17, 58 |
| Rule 33, Fed.R.Crim.P.. | 1-2, 5 |

OTHER

| | |
|---|----|
| ABA Formal Opinion 09-454. | 18 |
| United States Attorney’s Manual, §9-5.001(A) & (B)..... | 18 |

Introduction

This Reply Memorandum of Law is submitted on behalf of defendant Ross Ulbricht in support of his motions for a new trial pursuant to Rule 33, Fed.R.Crim.P., and to renew his motion(s) to suppress the fruits of certain searches and seizures performed by the government. In the intervening period since Mr. Ulbricht filed his Rule 33 motions, former Drug Enforcement Administration Special Agent Carl Force, as well as former Secret Service Special Agent Shaun Bridges, have been charged with offenses directly relating to the government's investigation of the Silk Road website, and directly related to this case.

During his summation, Assistant United States Attorney Serrin Turner disputed Mr. Ulbricht's defense, arguing that "[t]here were no little elves that put all of that evidence on the defendant's computer." T. 2166 (February 3, 2015).¹ Yet, as it turns out – and which AUSA Turner knew all along – there were indeed *two* "little elves" – law enforcement agents investigating the Silk Road website – operating secretly, illegally, corruptly, and brazenly even inside the Silk Road website itself. As the Complaint against former SA's Force and Bridges states, at 14, former SA Force "sought deliberately to undermine the integrity of the ongoing Baltimore Silk Road Task Force investigation."

As the record discussed below makes plain, by so doing, former SA Force, along with former SA Bridges, infected the integrity of the entire investigation of the Silk Road website. Yet Mr. Ulbricht was deprived not only of using that information in any manner, or to investigate it, but also of the capacity to use information the defense possessed *not* from the government's investigation of former SA Force, but from *discovery*.

¹ "T." refers to the trial transcript.

As detailed below, the charges against former SA's Force and Bridges reinforce Mr. Ulbricht's Rule 33 motions, not only because those charges provide additional exculpatory information that the government failed to disclose – indeed, the government did not disclose former SA Bridges's misconduct *at all* – as if in a case dominated by digital evidence the illegal conduct of the “computer forensics expert on the Baltimore investigation[,]” as the Complaint, at 3, describes him, would not be manifestly relevant – until the Complaint against him was unsealed – but also because the Complaint establishes that (a) the government was egregiously late in notifying the defense herein of the investigation and the underlying misconduct; and (b) that there was not any basis in the first place for keeping the investigation secret, as both former SA Force and former SA Bridges were acutely aware of the investigation and its particular subject matter for months prior to trial in this case.

Indeed, the only apparent reason for maintaining secrecy was to deprive Mr. Ulbricht of the use of the information, and to deny him Due Process, his Sixth Amendment rights to Compulsory Process and effective assistance of counsel, and, ultimately, a fair trial. Also, as detailed below, notwithstanding the government's conclusory refrain that the investigation of Mr. Ulbricht and that conducted by former SA's Force and Bridges were “independent,” the record irrefutably establishes otherwise. In fact, the investigations were coordinated and combined, with each sharing information generated by the other in a joint effort against the Silk Road web site.

Moreover, even if the investigations were not sufficiently connected, the information regarding former SA's Force and Bridges would still be relevant to this case. The government cannot sanitize the record of exculpatory material and information simply by trimming its trial

presentation to avoid mention of the offending law enforcement agents. Their misconduct qualifies as relevant independently of the government's case.

Throughout Mr. Ulbricht's trial the government repeatedly used the secret nature of the grand jury investigation as an excuse to preclude valuable defense evidence that was not only produced in discovery, independent of the investigation of Mr. Force. The government also worked aggressively to stymie the defense at every turn during trial when the defense tried to introduce favorable evidence. In that manner, the government improperly used the ongoing grand jury process in San Francisco as both a sword and a shield to deny Mr. Ulbricht access to and use of important evidence, to deprive the jury of essential facts, and to violate Mr. Ulbricht's constitutional rights to due process and a fair trial.

In addition to keeping any information about the investigation from the defense for seven months, then revealing it only five weeks prior to trial, and then moving to keep sealed and secret the general underlying information so that Mr. Ulbricht could not use it in his defense at trial, the government failed to disclose previously significant information included in the Complaint against former SA's Force and Bridges, including that *a second* federal law enforcement agent involved in the Silk Road investigation was corrupt and acting in concert with former SA Force.

Also, it is clear that former SA Force and others within the government obtained access to the administrative platforms of the Silk Road site, where they were able to commandeer accounts and had the capacity to change PIN numbers and other aspects of the site – all without the government's knowledge of what precisely they did with that access. In fact, as set forth below, the complete scope of what former SA's Force and Bridges were able to accomplish with

the illicit access they gained to the Silk Road web site, and its impact on this case, has yet to be determined.

In light of the information provided in the Complaint, it is now apparent to all just how relevant some of the issues raised by the defense at trial were, including the payment by Dread Pirate Roberts to a law enforcement agent for information about the investigation, the ramping up of the investigation of Mr. Ulbricht in mid-2013, soon after that paid information began flowing, and the creation of certain evidence at trial, such as the 2013 journal that conveniently begins – again – in Spring 2013, after the corruption alleged in this Complaint ripened.

As the evidence at trial – particularly from the government’s law enforcement witnesses – demonstrated, the Baltimore investigation and agents were inextricably involved in the evolution of the case and the evidence, as well as with alerting Mark Karpeles that he was under investigation, and meeting with his lawyers and exchanging information. At Mr. Ulbricht’s trial, knowing full well the corruption alleged in the Complaint made public today, the government still vigorously moved to preclude much of that evidence, kept it from the jury, and even had other similar evidence stricken from the record.

As discussed below, regarding the government’s claim that the information was not relevant, the government notified the defense of the investigation of former SA Force December 1, 2014. Two days later, the government provided its trial exhibits. Among those exhibits were several that referred to former SA Force in his various internet personas, including “Nob” (his authorized undercover alias), as well as his rogue identities on Silk Road, including alpacino, french maid, and Death From Above (all of which were providing, or attempting to provide, Dread Pirate Roberts with confidential information about the government’s investigation of Silk

Road). Thus, according to the government, even after it disclosed the fact of the investigation, it believed former SA Force was indeed quite relevant.

However, in the course of the ensuing litigation regarding whether the defense would be allowed to use the information about the investigation of former SA Force at Mr. Ulbricht's trial, by the time trial began the government either eliminated those exhibits or redacted them. During trial, the government successfully objected to the defense's attempts to introduce the unredacted documents the government had initially designated as its exhibits.

Yet in its Memo of Law opposing Mr. Ulbricht's Rule 33 motions, at 8, the government complains that "[n]or was there any other evidence presented by the defense, at any point during the trial," regarding the possibility of Mr. Karpeles controlling Silk Road. Given the government's unstinting efforts to prevent the defense from introducing any evidence about Mr. Karpeles, and to strike the testimony that was adduced, that position calls to mind the traditional attempt to provide an English translation for the Yiddish word *chutzpah*: a defendant who murders both his parents and then seeks mercy from the court because he is an orphan.

Accordingly, for all the reasons set forth above, as well as those previously set forth in prior litigation in this case, it is respectfully submitted that Mr. Ulbricht's Rule 33 motions for a new trial should be granted in their entirety. Alternatively, the Court should order and conduct the hearings requested below as to whether the Southern District of New York's investigation of the Silk Road website was, in fact, independent of the other federal investigations conducted during the same time frame, and as to what the government knew about former Special Agents Force and Bridges's authorized and unauthorized actions, and when they knew it.

STATEMENT OF THE FACTS

A dramatic event has occurred during the intervening period since Mr. Ulbricht's post-trial motions were filed. Less than two months after trial concluded in this case, the government filed criminal charges against former SA's Force and Bridges in the Northern District of California.

The Complaint against former SA's Force and Bridges (hereinafter the "Force Complaint") was unsealed March 30, 2015. A Department of Justice Press Release, March 30, 2015, "Former Federal Agents Charged With Bitcoin Money Laundering and Wire Fraud," available at <<http://www.justice.gov/opa/pr/former-federal-agents-charged-bitcoin-money-laundering-and-wire-fraud>>, summarized the Force Complaint's allegations against former SA Force as follows:

Force used fake online personas, and engaged in complex Bitcoin transactions to steal from the government and the targets of the investigation. Specifically, Force allegedly solicited and received digital currency as part of the investigation, but failed to report his receipt of the funds, and instead transferred the currency to his personal account. In one such transaction, Force allegedly sold information about the government's investigation to the target of the investigation.

As the Force Complaint itself notes, "[i]n late January 2013, members of the Baltimore Silk Road Task Force, to include BRIDGES and FORCE, gained access to a Silk Road administrator account as a result of the arrest of a former Silk Road employee." Force Complaint, at 5.

According to the Force Complaint, former SA Force "created certain fictitious personas" *id.*, at 3, and used those phony personas to "seek monetary payment, offering in exchange not to provide the government certain information." *Id.* Former SA Force also created fictional

characters, such as “Kevin,” a supposed law enforcement insider who was providing the information to Nob (who was former SA Force, in his authorized undercover role, masquerading as a drug dealer), which Nob in turn was corruptly providing to Dread Pirate Roberts (hereinafter “DPR”). *Id.*, at 14.

Also, former SA Force “stole and converted to his own personal use a sizable amount of bitcoins that DPR sent to Force . . .” *Id.*, at 4. Former SA Bridges also illegally acquired Bitcoin from the Silk Road website, and assisted former SA Force in his illegal endeavors. *Id.*, at 41-49.

In describing former SA Force’s assumption of the screen name DeathFromAbove, which he used alternately in an attempt to extort DPR, and/or provide inside law enforcement information to DPR, the Force Complaint concludes that former SA Force was the source of certain information in the LE_counterintel file found on Mr. Ulbricht’s laptop because the excerpts in that file “contain information that came from a person or persons inside law enforcement, in part because of their substance and in part because of their use of certain terminology and acronyms that are not widely know by the public.” Force Complaint, at 12.

As a result, in assessing former SA Force’s activities as DeathFromAbove, the Force Complaint posits that such misconduct “demonstrates that FORCE had a history of: (1) creating fictitious personas that he did not memorialize in his official reports or apprise his superiors at the DEA or the prosecutor of; (2) soliciting payments from DPR; (3) providing law-enforcement sensitive information to outside individuals when the disclosure of such information was not authorized and not memorialized in any official report.” *Id.*, at 26.

ARGUMENT

POINT I

**MR. ULBRICHT SHOULD BE GRANTED A NEW TRIAL
BECAUSE THE GOVERNMENT FAILED TO PROVIDE
EXCULPATORY MATERIAL AND INFORMATION IN A
TIMELY MANNER, THEREBY DENYING HIM HIS FIFTH
AMENDMENT RIGHT TO DUE PROCESS AND A FAIR TRIAL**

**A. *There Was Not Any Need to Maintain Secrecy of the Investigation
of Former SA's Force and Bridges Prior to Trial In This Case***

As a threshold matter, the Force Complaint reveals that the government's application prior to trial in this case to keep the investigation of former SA Force, and the information derived therein, secret was without any foundation.

As the Force Complaint demonstrates, both former SA Force and former SA Bridges were well aware of the investigation and its specific subject matter. For example, as the Force Complaint states, Force resigned from the DEA May 4, 2014, "shortly after law enforcement began the current investigation." Force Complaint, at 7, 35. Days later, May 8, 2014, former SA Force wired \$235,000 to an offshore account in Panama, with the Complaint noting that he did so "presumably after learning of the government's investigation and after he had resigned[.]" *Id.*, at 39.

In fact, former SA Force even voluntarily submitted to an interview by law enforcement that his lawyer suggested. *Id.*, at 40. That meeting occurred May 30, 2014, *id.*, a full six months before the defense was notified of former SA Force's misconduct. Similarly, former SA Bridges was interviewed (with counsel) by law enforcement more than once, including November 13, 2014, eight days before the government wrote the Court in this case. *See Id.*, at 47-48.

In addition, the government inexcusably waited seven months before informing the defense of the misconduct by former SA Force – and never did prior to trial with respect to

former SA Bridges. As the Complaint notes, the United States Attorney’s Office for the Northern District of California opened its investigation of former SA Force May 2, 2014. *See* Force Complaint, at 47. Two days later, DoJ’s Public Integrity Section opened an official investigation of him. *Id.*

Nor were there any facts in the Complaint that were not entirely established well before the government notified the defense in this case, much less before trial herein. The last misconduct allegedly occurred in mid-2014. Thus, there was not any basis for maintaining secrecy other than to impair Mr. Ulbricht’s defense through precluding not only his use of the information, but even his ability to investigate it.

B. *The Government Continues to Misapprehend Its Obligation to Produce Exculpatory Material and Information to the Defense*

The government’s claim, in its Memo of Law, at 3, that it “timely disclosed to the defense in the agent’s 3500 material” (produced pursuant to 18 U.S.C. §3500) certain exculpatory material completely avoids confronting the legion of cases admonishing the government that production of 3500 material on the eve trial – here 5,000 pages for the first witness alone – is not a substitute for disclosure of material pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963).

As the Second Circuit emphasized in *United States v. Rodriguez*, 496 F.3d 221 (2d Cir. 2007),

Brady information must be disclosed, furthermore, in a manner that gives the defendant a reasonable opportunity either to use the evidence in the trial or to use the information to obtain evidence for use in the trial. Thus, the Government must make disclosures in sufficient time that the defendant will have a reasonable opportunity to act upon the information efficaciously. *See Leka [v. Portuondo*, 257 F.3d 89,] 100 (2d Cir. 2001) (noting that *Brady*

disclosures must be timed so that the defense has a sufficient opportunity to use them) . . . Similarly, disclosures must be sufficiently specific and complete to be useful. *See Leka*, 257 F.3d at 103 (finding *Brady* not satisfied where Government did not disclose details of potential witness's knowledge, because defendant was left to gamble on what witness would say).

496 F.3d at 225-26.

Similarly, in *United States v. Rittweger*, 524 F.3d 171 (2d Cir. 2008), the Circuit, noting that “[t]he government produced Allen's grand jury testimony pursuant to its obligations under the Jencks Act, 18 U.S.C. § 3500[.]” reiterated that

[c]omplying with the Jencks Act, of course, does not shield the government from its independent obligation to timely produce exculpatory material under *Brady* – a constitutional requirement that trumps the statutory power of 18 U.S.C. § 3500. *See Rodriguez*, 496 F.3d at 225-26 (recognizing independence of obligations under Jencks Act and *Brady*).

524 F.3d at 181 n.4. *See also United States v. Coppa*, 267 F.3d 132, 145-46 (2d Cir. 2001) (in discussing the relative authority of *Brady* and 18 U.S.C. §3500, noting that “of course, a fundamental axiom of American law, rooted in our history as a people and requiring no citations to authority, that the requirements of the Constitution prevail over a statute in the event of a conflict”).

Thus, in *United States v. Jacobs*, 650 F. Supp. 2d 160 (D. Conn. 2009), the District Court cautioned the government that

[i]f the statements made by co-conspirators are material within the meaning of *Brady* and its progeny, it is not enough that they “will be provided in accordance with the Jencks Act.” Gov’t Resp. at 7. I remind the government again that its *Brady* obligations trump the Jencks Act, *Rittweger*, 524 F.3d at 181 n. 4, that such obligations include the obligation to produce impeachment materials consistent with *Giglio* [*v. United States*, 405 U.S. 150 (1972)], *see Coppa*, 267 F.3d at 139, and that such material must be produced

“in time for its effective use at trial.” *Id.* at 135, 142.

650 F. Supp.2d at 171.

Similarly, the government’s contention, in its Memo of Law, at at 18-19, that production of 3500 material “nearly two weeks before trial began[]” without noting that the volume for the first witness alone – Homeland Security Investigations Special Agent Jared D. Der-Yeghiayan – was *5,000 pages*, fails to appreciate at all the purpose behind *Brady* and the substance of the prosecutor’s obligations.

Also during that time prior to trial the government also repeatedly modified its exhibits in a manner that required constant adjustment by the defense. While the government, in its Memo of Law, at 20 n. 6, asserts that its changes involved “adding metadata,” metadata was in many respects the essence of the government’s evidentiary presentation.

As excerpted below from the “Government Exhibit Additions, Modifications, and Deletions Chart,” attached as Exhibit 2 to Mr. Ulbricht’s post-trial motions filed March 6, 2015 (Docket #223), the changes the government made to its exhibits from December 31, 2014 (when the first 3500 material was produced), until trial began, were neither “minor” nor “nonsubstantive,” as the government claims. *Id.*

| | |
|---------|--|
| 1/02/14 | The government provides new Rule 16 discovery: voicemails from Ross Ulbricht to Richard Bates (one of which later becomes GX 1005). |
| 1/07/15 | The government makes major revisions to exhibits, which are too numerous to be provided by email. The government does not provide any indication by email, phone or otherwise indicating which exhibits have been deleted, which have been modified or renumbered, and/or which descriptions were changed in the exhibit list. |
| 1/08/15 | The government provides new disk with 900 series added. |
| 1/08/15 | At defense counsel’s request, AUSA Serrin Turner sends an email explaining |

changes made to the exhibits contained in the new disks provided to counsel on 1/07/15 and 1/08/15, which are as follows:

New exhibits:

100A
 100B
 106(D)
 107(D)
 117A
 118A-C
 121A
 124
 128B-J
 129A
 131
 132
 201B, I, & J
 213
 214
 242
 290
 291
 301
 304
 311
 316
 500A
 501D
 600
 603/603A
 604/604A
 700-704 are new (703 is an updated version of what was formerly 700)
 804

900 series is all new except for 920A-936. However, the gist of the new exhibits is the same as the exhibits formerly in the latter half of the 200 series (which have been removed and replaced with these) – i.e., screenshots and transactional data taken from the SR server.

1000 series consists of google chats formerly in 300 series, except 1000 is new

Other changes:

Metadata has been added to many of the exhibits in the 100 & 200 series
Some of the exhibits have simply been renumbered

Torchat changes:

The torchats in the new list (222-232D) largely overlap with (and replace) the torchats that were included in the prior exhibit list. However, the chats have been broken up into smaller excerpts (or related sets of excerpts), with each made into a separate exhibit. Additionally, some material has been deleted from the chats; and some exhibits contain new chat excerpts not included in our earlier set of exhibits.

Defense counsel also discovers that the government has removed 31 exhibits contained in their initial exhibit list, as follows:

Removed Exhibits:

111(D) — Example of BTC address and example of Private Key
116(D) — Bestselling jewelry
116(E) — bestselling apparel
116(F) — pill press.
116(G) — book on silencers etc.
116(H) Book excerpts on making c-4,
122 — 4 steps to get customer help
123 — A few words from DPR — now just DPR profile
125EE — SR gets a new look
125F — SR Forum Post : withdrawal problems;
125M — Stealth mode feature for vendors
125O — response to bitfool claiming DPR is doing this for the money
126B — private messages between DPR, Cirrus, SSBD re: mod powers
210 — removal of screenshot of Root directory on Ulbricbht laptop
217 — Screenshot backup coin folder
220 — Torchat buddy list
240D — 1-1-12 journal entry from Laptop
243 — Log of detected efforts of LE to investigate SR
252 — Document regarding planned SR upgrades
258 — Statement of DPR to SR community regarding DDOS attack on website
259 — Document detailing user purchase process on SR
276 A-F
277 A-D

Defense counsel also discovers that the government has added the following additional exhibits, not noted by the government in the summary provided:

| | |
|---------|--|
| | <p><u>Additional Exhibits:</u></p> <p>200A — screenshot of Hash for Ross’s laptop 201 series — chosen a few new 222 — Complete log file of SSH torchat 231A-C — Torchats with Smed 602 — Server photograph</p> |
| 1/10/15 | Government adds 3 new exhibits (GXs 226F, 125G and 212A), modifies and makes additions to 3 others (GX 113: page added; GX 118B: metadata corrected; GX 936: messages from Silk Road forum added), and adds stickers to two existing exhibits (GXs 240C and 914) |
| 1/12/15 | <p>Emails from Serrin Turner include 5 new exhibits and 13 modified exhibits:</p> <p><u>New Exhibits:</u></p> <p>GX 111 (screenshot of crack cocaine page, which is the same as the first page of GX 103B) GX 133 (a screenshot of the DPR public key listed on the Silk Road website) 3 demonstratives: GX 106A - who.is lookup of nfl.com GX 106B - who.is lookup of .onion site GX 107A - close up of screen from end of GX 107 video)</p> <p><u>Modified Exhibits:</u></p> <p>GX 102D: pages added GX 212A: pages deleted GX 291: redactions removed GX 201B, 201H, 201I: timezone of metadata changed GX 930 - 936: time zone changed to GMT</p> |

Nor should the impact of “breaking up pages of documents into separate exhibits or adding metadata” be minimized with respect to Mr. Ulbricht’s ability to prepare for trial with the exhibits provided. The constant reordering, renumbering and subdividing made it nearly impossible for defense counsel to keep up with what information was contained in which exhibit (and thus which exhibits would be most pertinent during trial). Moreover, in this computer data-centric case the metadata underlying a particular exhibit was, in many instances, more important

than the exhibit itself.

In addition, the government's argument, in its Memo of Law, at 19, that the defense was able to use the 3500 during cross-examination further demonstrates the government's failure to understand its *Brady* obligations. The fact that the defense was able to read the documents and integrate them into cross-examination of SA Der-Yeghiayan – much of which was stymied by the government's objections that profited significantly from its preclusion of the information regarding former SA Force – is the equivalent of timely *Brady* disclosure that would permit adequate investigation of the information, and development of admissible evidence. *See United States v. Gil*, 297 F.3d 93, 105-06 (2d Cir. 2002); *Leka v. Portuondo*, 257 F.3d 89, 101 (2d Cir. 2001) (“[t]he limited *Brady* material disclosed to [the petitioner] could have led to specific exculpatory information only if the defense undertook further investigation. When such a disclosure is first made on the eve of trial, or when trial is under way, the opportunity to use it may be impaired. The defense may be unable to divert resources from other initiatives and obligations that are or may seem more pressing. And the defense may be unable to assimilate the information into its case”), *citing United States v. Cobb*, 271 F. Supp. 159, 163 (S.D.N.Y.1967) (Mansfield, J.) (“there may be instances where disclosure of exculpatory evidence for the first time during trial would be too late to enable the defendant to use it effectively in his own defense, particularly if it were to open the door to witnesses or documents requiring time to be marshalled and presented.”). *See also* Mr. Ulbricht's initial post-trial Memo of Law, at 7-9.

That is why the government's persistent conflation of its distinct *Brady* and Jencks Act

obligations has been so often criticized. *See ante*, at 9-10, 15. *See also* Mr. Ulbricht's initial post-trial Memo of Law, at 9-11. Nor, given the repeated attention to the issue, could the government's continued failure to acknowledge that those two duties are distinguishable be the product of ignorance or confusion.

Moreover, the government's rationale, in its Memo of Law, at 10, n. 1, regarding why it failed to apprise the defense of the involvement of a *second* law enforcement agent (former SA Bridges) in corrupt and illegal activities in relation to the Silk Road site is entirely specious. That former SA Bridges's involvement was not known until after the government's November 21, 2014, letter was submitted does not absolve the government of a continuing disclosure obligation that continues even today. *See, e.g., Leka v. Portuondo*, 257 F.3d 89, 100 (2d Cir. 2001) ("[i]ndeed, *Brady* requires disclosure of information that the prosecution acquires during the trial itself, or even afterward"), *citing Imbler v. Pachtman*, 424 U.S. 409, 427 n. 25 (1976) (noting that the duty to make *Brady* disclosures at trial "is enforced by the requirements of due process"). *See also Poventud v. City of New York*, 750 F.3d 121, 176 (2d Cir. 2014).

Also, as pointed out above, at 8, former SA Bridges was interviewed twice prior to the government's November 21, 2014, letter to defense counsel, and was already the subject of the inquiry that resulted in the charges filed recently. Consequently, the government – especially in the *Brady* context – certainly knew, should have known, or had reason to know of the investigation of former SA Bridges and his relationship to former SA Force's misconduct.

The government's manifest dereliction with respect to its obligations to produce exculpatory material and information is also demonstrated by its repetition, in its Memo of Law, at 11, of the canard that it initially disclosed the information about the investigation of former

SA Force, and his misconduct, “in an abundance of caution.”

That is pure sophistry. There is not an “abundance of caution” principle in criminal discovery. Rule 16 does not include any “abundance of caution” clause or discovery obligation; nor does *Brady*. The government disclosed the information because it recognized that if it did not, and former SA Force was subsequently charged, it would be obvious and incontrovertible that it had withheld exculpatory material it should have disclosed.

Thus, eight months into the investigation, and only six weeks prior to trial, the government disclosed – although, as the Court noted in the December 15, 2014, (then-sealed) pretrial conference, the government’s motion to invoke Rule 6(e), Fed.R.Crim.P., to preclude the defense’s use, admission, or even investigation of the information was tantamount to not disclosing *at all*. See Transcript, December 15, 2014, at 48.²

The reasons for the government’s refusal to acknowledge that its disclosure constituted *Brady* material are sufficiently obvious that they need not be explained further. However, that does not excuse it, or alter the facts. Indeed, a recent report by the National Association of Criminal Defense Lawyers (hereinafter “NACDL”), *Material Indifference: How Courts Are Impeding Fair Disclosure in Criminal Cases*, available at <<http://www.nacdl.org/discovery/reform/materialindifference/>> (hereinafter “NACDL Report”), which reviewed 620 decisions deciding the merits of an alleged *Brady* violation, found that “[t]he judiciary’s almost unilateral

² At the December 15, 2014, pretrial conference, during the then-sealed portion, the Court recognized, in colloquy with the government, “so it’s as if the disclosure never occurred. Because in fact it’s even more frustrating, because they have information that’s been put in their pocket, if you will, so that government can say you disclosed it, but they can’t use any of it, that includes the most basic information, which is just Carl Force under investigation.” Transcript, December 15, 2014, at 48.

focus on materiality conveys a message that non-material favorable information is unimportant and need not be disclosed. As a result, the current system of judicial review fails to promote a culture of compliance, instead fostering *Brady*, or ‘so-called *Brady*,’ violations.” NACDL Report, at 44.³

As a result, the NACDL Report concluded, regardless of whether the courts found a *Brady* violation (which they hardly ever did), the “important point is that valuable information that could have helped bolster the defense theory, led to a more effective trial strategy, or led to other material information was not turned over to the defense.” *Id.*, at 42. Here, that systemic problem was exacerbated by Assistant United States Attorney Serrin Turner’s assertion, to defense counsel in a December 2014 telephone conversation, that “there is no *Brady* material because [Mr. Ulbricht] is very, very guilty.” Given that approach to the government’s constitutional obligations – depending whether the prosecutor believes the defendant is guilty of the charges that prosecutor has instituted – it is of course *impossible* for *any* information or material to be viewed as exculpatory, or acknowledged as same. Conveniently, that concurrently absolves a prosecutor of any obligation to produce *any* material pursuant to *Brady*. See *United States v. Rittweger*, 524 F.3d 171, 181-82 (2d Cir. 2008).

³ As the NACDL Report points out, prosecutors’ inability to recognize the character of material and information they have a duty to disclose is at odds with their ethical obligations, but nevertheless fostered by prosecutorial doctrine that is in conflict with those ethical duties. While courts have “been reminding prosecutors all along that they are ethically bound under professional rules to a broader disclosure obligation beyond what the Constitution provides a defendant[,]” NACDL Report, at 8, *citing* ABA Formal Opinion 09-454 (“requires the disclosure of evidence or information favorable to the defense without regard to the anticipated impact of the evidence or information on a trial’s outcome”), the United States Attorney’s Manual, at §9-5.001[A] & [B], focuses the prosecutorial disclosure obligation instead on the concept of “materiality,” advising that “ordinarily[] evidence that would not be admissible at trial need not be disclosed”). See also *Cone v. Bell*, 556 U.S. 449, 470 n.15 (2009).

In that context, the government's response, in its Memo of Law, at 22 n. 7, with respect to the inexplicable redaction of Anand Athavale's name and certain information about him from SA Der-Yeghiayan's 3500 material, *see* 3505-3722; *see also* Mr. Ulbricht's Initial Memo of Law in Support of His Post-Trial Motions (hereinafter "Initial Memo of Law"), at 11, further establishes that the government does not possess a reliable appreciation of what constitutes exculpatory material and information. That one reviewer would *not* redact the very same information that another (or even the same) reviewer would redact from another document provides little assurance that other exculpatory information was not also redacted improperly. Indeed, it produces the opposite conclusion and concern: that over-redaction deprived the defense of additional exculpatory information within the 3500 material.

The government also grossly misconstrues its obligations under *Brady* by claiming that SA Force's unreported misconduct was not subject to production by *him* (and by former SA Bridges with respect to his misconduct as well), and that such nondisclosure is attributable to the government. Indeed, the government cannot cite a case for the proposition that unauthorized (mis)conduct by law enforcement is somehow exempt from *Brady*.

That defies logic, as it suggests that all a law enforcement officer has to do to avoid the government's disclosure obligation is to commit misconduct and not disclose. For instance, if a police officer plants a weapon or drugs on a defendant for purposes of arresting and charging him, that is *Brady* material regardless whether the prosecutor knew of it and/or suppressed it deliberately or unknowingly.

Contrary to the government's uninformed contention, its *Brady* obligations exist regardless whether the non-disclosure is deliberate or inadvertent. *See, e.g., Strickler v. Greene*,

527 U.S. 263, 280-81, 288 (1999); *United States v. Jackson*, 345 F.3d 59, 73 (2d Cir. 2003) (“[u]nder *Brady*, ‘[t]he individual prosecutor is presumed to have knowledge of all information gathered in connection with the government’s investigation,’ and ‘the prosecutor’s good faith or lack of bad faith is irrelevant’”), *quoting United States v. Payne*, 63 F.3d 1200, 1208 (2d Cir.1995). *See also Poventud v. City of New York*, 750 F.3d 121, 182-83 (2d Cir. 2014).

The prosecutor’s responsibility is also not merely personal, but encompasses the entire prosecution team, which is construed rather broadly to include anyone involved in the government investigation. *See, e.g., United States v. Bin Laden*, 397 F. Supp. 2d 465, 481-84 (S.D.N.Y. 2005) *aff’d sub nom. In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 93 (2d Cir. 2008), *citing United States v. Bufalino*, 576 F.2d 446, 448-50 (2d Cir.1978).

In fact, in *Bin Laden*, the U.S. Marshals handling witness security issues made unauthorized videotapes of witness interviews *unbeknownst* to the AUSA’s involved in the case. Yet even that limited role did not exclude them from the prosecution team, or alleviate the government’s disclosure responsibilities under *Brady*. 397 F. Supp.2d, at 481.⁴

⁴ Again failing to comprehend the nature of exculpatory material and information, the government, in its Memo of Law, at 16 n. 5, cannot discern the exculpatory character of the 3500 material for Special Agent Alford enumerated in Mr. Ulbricht’s initial Memo of Law. However, in 3501-206, SA Alford’s September 27, 2013, communication, he notes that “[i]nterviews were obtained after the takedown of SR in various parts of the country by IRS and DEA counterparts upon the direction of SA Alford.” That such interviews did not (with perhaps the exception of Richard Bates) produce anything that incriminated Mr. Ulbricht permits the converse inference: that at least some portion of those interviews produced exculpatory information or statements by those persons interviewed.

C. *The Government’s Investigations of Mark Karpeles and Anand Athavale Were Not Mere “Leads” or “Theories” or “Suspensions” or “Hunches”*

In a further effort to excuse its late production of *Brady* material in the guise of 3500 material on the eve of trial, the government’s cites, in its Memo of Law, at 18, cases for the proposition that the “prosecution is not required under *Brady* to disclose every lead, theory, suspicion, or hunch entertained by law enforcement agents during their investigation.” Yet those cases are patently inapposite.

1. *The Government’s Investigation of Mark Karpeles*

SA Der-Yeghiayan’s investigation of Mark Karpeles was not a “lead, theory, suspicion, or hunch[.]” Rather, as SA Der-Yeghiayan’s 3500 material demonstrates, he swore *two* separate affidavits in support of search warrants for Mr. Karpeles’s e-mail accounts, in two different federal districts, over the course of several months, attesting that there was *probable cause* to believe that Mr. Karpeles was engaged in criminal activity related to operating or managing the Silk Road website.⁵

In a May 29, 2013, e-mail from SA Der-Yeghiayan, he attaches a draft affidavit for a search warrant in the Northern District of Illinois. *See* 3505-13 (attached hereto as part of Exhibit 1). Within that affidavit, SA Der-Yeghiayan declares that

[b]ased on the above information, I believe there is probable cause that the email address magictux@gmail.com and the email address mark@tibanne.com will contain information and evidence related to the distribution can [sic] of controlled substances and conspiracy to distribute a controlled substance as well as additional evidence of KARPELES operating as an unlicensed money service

⁵ Of course, as discussed **post**, at 45-48, that also inextricably links the various federal investigations, including the Baltimore investigation, of the Silk Road site, and demonstrates the relevance of former SA’s Force and Bridges’s misconduct to *this* case.

business.”

See 3505-20-21 (attached hereto as part of Exhibit 1). *See also* 3505-24-25 (relating to the investigation of Mr. Karpeles and his Bitcoin exchange company, Mt. Gox).

Nearly three months later, August 15, 2013, SA Der-Yeghiayan performed the same function for the *Southern District of New York*. In an e-mail that day to AUSA Turner, SA Der-Yeghiayan noted he was “preparing to swear this out today.” *See* 3505-205 (attached hereto as part of Exhibit 2). Attached to that e-mail, which was in response to an e-mail from AUSA Turner earlier that day, with the draft affidavit attached (and which was most likely written by AUSA Turner). *Id.*

In the affidavit, at 3505-206-33 (attached hereto as part of Exhibit 2), SA Der-Jeghiayan swears that “there is probable cause to believe that the SUBJECT ACCOUNTS contain evidence, fruits, and instrumentalities of narcotics trafficking and money laundering, . . .” 3505-209-10 (at ¶ 3). *See also* 3505-226, at ¶ 23 (“I respectfully submit there is probable cause to believe that KARPELES has engaged in the SUBJECT OFFENSES”).

The affidavit by SA Der-Yeghiayan, ostensibly written by AUSA Turner, states that it is “based on my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers and civilian witnesses.” 3505-210 at ¶ 4 (Exhibit 2). Also, it “does not include all the facts that I have learned during the course of my investigation.” *Id.*, at ¶ 4.

Specifically, the affidavit also attests that:

- “I believe that KARPELES has been involved in establishing and operating the Silk Road website.” 3505-224, ¶ 22. *See also* 3505-267 (July 11, 2012, e-mail from SA Der-Yeghiayan stating, “[w]e think we found out who’s behind the [Silk Road]”);
- Mr. Karpeles “has the technical expertise and experience necessary in order to establish and operate a large commercial website such as the Silk Road Underground Website.” 3505-225, at ¶ 22(c);
- Silk Road “relies on a highly complex system for processing Bitcoins strongly suggests that it was designed by someone with extensive technical expertise related to Bitcoins – which KARPELES, being the owner and operator of a major Bitcoin exchange and Bitcoin discussion forum, clearly has.” *Id.*; and
- “. . . in early 2011, around the same time the Silk Road began operating, KARPELES acquired Mt. Gox. Given his ownership of this Bitcoin exchange business, KARPELES had a strong motive to create a large underground marketplace where Bitcoins would be in high demand. The Silk Road website was uniquely well suited to this purpose, as it generated a huge source of demand for Bitcoins. Indeed, as of April 2013, the total value of Bitcoins in circulation topped 1 billion dollars. Because there few legitimate vendors who accept Bitcoins as payment, it is widely believed that the rise of Bitcoins has been driven

in large part by their use on Silk Road.” 3505-224-25, at ¶ 22(b).⁶

As part of the SDNY search warrant application, AUSA Turner himself filed a declaration seeking a Sealing Order, in which he affirmed that sealing was necessary “to avoid premature disclosure of the investigation which could inform potential criminal targets of law enforcement interest[.]” 3505-234 (attached as part of Exhibit 2). Thus, AUSA Turner asked the Magistrate Judge to “order the Provider not to notify any person of the existence of the warrant.”⁷

Notwithstanding these facts, the government possesses the temerity to describe the investigation of Mr. Karpeles – and the rationale for not disclosing it as *Brady* material – as a “hunch” or “lead” or “theory” or “suspicion.” *Probable cause*, determined by the very same prosecutor who tried this case, is exceedingly more substantial than of those ephemeral concepts.

In addition, the government’s claim, in its Memo of Law, at 17, that the investigation shifted to Mr. Ulbricht once he was identified as a suspect is again refuted by the record created

⁶ In an undated report, SA Der-Yeghiayan also stated, “Agents have discovered strong ties between those controlling the bitcoin markets and those operating the Silk Road.” 3505-3122-24. *See also id.*, (“HSI O’Hare has also identified multiple financial accounts belonging to the Silk Road operators which contain bitcoins equal in value to millions of U.S. dollars” and “[o]ver the last few months, HSI O’Hare has made several breakthroughs in identifying high priority targets believed to be the backbone of the website”). SA Der-Yeghiayan also wrote another, six-page report regarding his then-ongoing investigation of Mr. Karpeles. *See* 3505-3475-80.

⁷ That concern about notice related to Mr. Karpeles and his confederates, and not to Mr. Ulbricht, who was not yet a target or even focus of the government’s investigation and is not even mentioned in the warrant application. Of course, as discussed **post**, at 56, Mr. Karpeles had already been alerted to U.S. law enforcement’s interest in him by the precipitous seizure – by none other than former SA Bridges (likely in concert with former SA Force) – of Mr. Karpeles’s accounts at Dwolla, a money exchange business, worth more than \$2 million dollars.

by the government itself. For example, September 30, 2013, the day before Mr. Ulbricht's arrest,

SA Der-Yeghiayan requested, "can we also have a copy of their UC chats (and their Seattle counterparts) with DPR to see if there's any language or connections to [Mr. Karpeles] or the vendors we're working." 3505-3512.

The day after Mr. Ulbricht's arrest, October 2, 2013, SA Der-Yeghiayan wrote an e-mail that "after reviewing some notes from [Mr. Ulbricht's] computer last night/this morning there appears to be some inferences to [Mr. Karpeles's] involvement and associations to [Silk Road]." 3505-3020. Also, SA Der-Yeghiayan wrote in an October 7, 2013, e-mail – nearly a week after Mr. Ulbricht's arrest – to AUSA Turner and Internal Revenue Service Special Agent Gary Alford, in response to SA Alford's e-mail regarding an allegedly hacking of the bitcoin forum soon after Mr. Ulbricht's arrest, "I figured MK [Mr. Karpeles] is purging everything after [Mr. Ulbricht's] arrest . . . I know he was initially involved." 3505-707 (ellipsis in original).

A week later, in an October 15, 2013, e-mail, SA Der-Yeghiayan was still providing materials relating to Mr. Karpeles, as he sent AUSA Turner an Excel spreadsheet of "Karpeles Dwolla Transactions" – which consists of nearly one thousand pages. *See* 3505-895, 901-2916. SA Der-Yeghiayan also authored an investigative report dated October 17, 2013, a little more than two weeks after Mr. Ulbricht's arrest, regarding the return on a search warrant served on Google for two of Mr. Karpeles's e-mail accounts. *See* 3505-3869.

At the same time, the government was also reaching out to Mr. Karpeles for information about Mr. Ulbricht. In an October 12, 2013, e-mail to AUSA Turner and SA Alford, SA Der-Yeghiayan, commenting on the source of information about Mr. Ulbricht's Mt. Gox account,

“just heard that information was passed from MK’s [Mark Karpeles’s] atty’s to Baltimore.” 3505-895.

Thus, Mr. Karpeles was a subject of the government’s investigation from mid-2012 (*see* 3505-267, cited *ante*, at 23) – nearly 18 months – until even after Mr. Ulbricht’s arrest, which ultimately occupied the entirety of the prosecution’s attention. In fact, as SA Der-Yeghiayan confirmed at trial, the government has never examined any of Mr. Karpeles’s electronic devices, or servers, or any of his other e-mail accounts beyond the two covered by the subpoena served upon Google. T. 681-82.

Consequently, the government’s claim that its investigation of Mr. Karpeles was insufficiently substantive to constitute exculpatory material and information it was required to disclose is simply unsustainable.

2. *The Government’s Investigation of Anand Athavale*

The government’s investigation of Anand Athavale also constituted an inquiry far more substantial than a “hunch,” “lead,” “theory,” or “suspicion.” In a November 12, 2012, e-mail, SA Der-Yeghiayan wrote that “[w]e believe we just make a break through recently and have identified the administrator of the website who is residing in or around Vancouver.” 3505-318.

The next day, November 13, 2012, SA Der-Yeghiayan described Mr. Athavale at “the target,” 3505-316, and “the Vancouver target.” 3505-317. *See also* 3505-738-39 (November 19, 2012, e-mail from SA Der-Yeghiayan stating, “[t]his guy I believe [] is the main admin for the website”). SA Der-Yeghiayan would later write, too, that Mr. Athavale “has the computer skills and knowledge to [be] able to operate the Silk Road in the manner in which it appears DPR does[,]” and “has demonstrated the ability to be able to play the part of multiple identities

online.” 3505-3084.

In that November 13, 2012, e-mail, SA Der-Yeghiayan also reported that “[w]e also have pages of chats conducted with a UC agent. I took all the chats and message created by the user and was searching key words used by the administrator in another online forum I believe the Admin posts in.” 3505-316. Elaborating, SA Der-Yeghiayan explained that he had “spent quite a bit of time analyzing his writing and posts he has made. Even went as far as having an English professor from a major University critique each writing sample[] and who said they could very well be the same person.” 3505-317.

SA Der-Yeghiayan prepared a ten-page report regarding his investigation of Mr. Athavale, focusing on Mr. Athavale’s background, his extensive internet presence, and a comparison of Mr. Athavale’s writing style with that of Dread Pirate Roberts. 3505-591-600 (a copy of which is attached as Exhibit 3). That analysis included 32 separate similarities cited by SA Der-Yeghiayan. 3505-596-97.

SA Der-Yeghiayan’s report regarding Mr. Athavale also noted that “HSI O’Hare has identified ATHAVALÉ as the likely identity behind the SR [Silk Road] administrator username Dread Pirate Roberts by using the posts on the SR Forum, and using the chat sessions recorded by HSI Baltimore.” 3505-598. SA Der-Yeghiayan’s report explained that “[t]here has been extensive analysis of distinct writing styles, sayings, spelling mistakes, cliches and specific nuances, which have led to determining ATHAVALÉ as *a highly likeable target*.” *Id.* (emphasis added). Also, HSI O’Hare formally requested the assistance of HSI Vancouver (where Mr. Athavale reportedly resided) in the investigation of Mr. Athavale. *Id.*

In another report regarding Mr. Athavale, SA Der-Yeghiayan set forth in six pages of detail, with specific examples, 27 separate similarities “in use of words or statements” made by Mr. Athavale and DPR. 3505-3072-78, as well as lengthy passages from posts made Mr. Athavale. 3505-3078-83.

The government’s attempts, in its Memo of Law, at 18, to minimize the importance of SA Der Yeghiayan analysis of language patterns in identifying DPR would be merely unavailing if they were not so disingenuous and contrary to the government’s professed investigative purposes with respect to Mr. Ulbricht.

For example, the warrant for Mr. Ulbricht’s laptop (attached as Exhibit 11 to the August 1, 2014, Affidavit of Joshua L. Dratel, Esq., in support of Mr. Ulbricht’s motion to suppress certain evidence) sought, and received, authorization to search for precisely that information:

44. The SUBJECT COMPUTER is also likely to contain evidence concerning ULBRICHT relevant to the investigation of the SUBJECT OFFENSES, including evidence relevant to corroborating the identification of ULBRICHT as the Silk Road user "Dread Pirate Roberts," including but not limited to:
 - a. any communications or writings by Ulbricht, which may reflect linguistic patterns or idiosyncracies associated with “Dread Pirate Roberts”[] or political/economic views associated with “Dread Pirate Roberts” (*e.g.*, views associated with the Mises Institute);

* * *
 - c. any evidence concerning Ulbricht's travel or patterns of movement, to allow comparison with patterns of online activity of “Dread Pirate Roberts” and any information known about his location at particular times;

* * *
 - h. any other evidence implicating ULBRICHT in the SUBJECT OFFENSES.

See ¶ 44 of the Application for a Search Warrant for Mr. Ulbricht’s laptop.

The footnote to ¶ 44(a) explained the basis for that blanket search:

For example, “Dread Pirate Roberts” is known often to begin sentences with “Yea” – distinct from the usual spelling of the word, “Yeah.” ULBRICHT is also known to favor this spelling of the word; for instance, his username on YouTube is “ohyeaross.” The SUBJECT PREMISES is expected to contain writings or communications that will allow for similar linguistic comparisons between ULBRICHT and “Dread Pirate Roberts.”

Id., at ¶ 44(a) n. 21.

In fact, the government prepared (but did not use) for SA Der-Yeghiayan’s re-direct examination at trial a series of exhibits highlighting, with red circles, that alleged idiosyncrasy in various electronic communications. Thus, again, the government’s argument is contradicted dispositively by its own investigative priorities and its trial preparation.

Thus, SA Der-Yeghiayan devoted countless hours examining Mr. Athavale’s language patterns, and ultimately a series of pages in his reports to the subject, and even submitted all the material to a college professor for expert analysis, with the professor reporting back that Mr. Athavale and DPR “could very well be the same person.” 3505-317.

It is assumed, based on the search warrant application for Mr. Ulbricht’s laptop and social media accounts, as well as the prospective government exhibits at trial, that SA Der-Yeghiayan and/or other agents and AUSA’s performed the same meticulous scrutiny with respect to Mr. Ulbricht’s communications. Yet no such opinion by a college professor or anyone else was provided to the defense with respect to Mr. Ulbricht.

Moreover, SA Der-Yeghiayan’s interest in Mr. Athavale remained active until at least April 2013 – well after former SA Force, in his guise as DeathFromAbove, had alerted DPR that the government believed he was Mr. Athavale – as evidenced by subsequent e-mails from SA

Der-Yeghiayan. *See* 3505-3057-58 (e-mails dated April 3, 2013 & April 4, 2013).

Thus, Mr. Athavale represented not a “hunch” or “lead,” but rather, as described by the Special Agent with the most law enforcement experience monitoring and studying the Silk Road website, was “a highly likeable target” to whom significant investigative resources were devoted, including numerous hours of SA Der-Yeghiayan’s time, for at least five months. It bears noting as well that, as is the case with Mr. Karpeles, the government has never examined Mr.

Athavale’s electronic devices or his e-mail accounts, or the contents of the various servers and internet domains he has controlled. T. 682.

Judge Alex Kozinski, dissenting in *United States v. Olsen*, 737 F.3d 625 (9th Cir. 2013), announced that “[t]here is an epidemic of *Brady* violations abroad in the land[,]” and that “[o]nly judges can put a stop to it.” *Id.*, at 626 (Kozinski, J., *dissenting*). *See also id.*, at 631-32 (“*Brady* violations have reached epidemic proportions in recent years, and the federal and state reporters bear testament to this unsettling trend”) (citations omitted).

Judge Kozinski added that “[a] robust and rigorously enforced *Brady* rule is imperative because all the incentives prosecutors confront encourage them not to discover or disclose exculpatory evidence . . .” *Id.*, at 630. As a result, Judge Kozinski urged his judicial colleagues that they “must send prosecutors a clear message: Betray *Brady*, give short shrift to *Giglio*, and you will lose your ill-gotten conviction.” *Id.*, at 633.

D. *The Information That Was Not Disclosed Until the Force Complaint Was Unsealed*

The Force Complaint also revealed information that was not previously disclosed by the government. Obviously, the most dramatic was the involvement of a second law enforcement agent, former SA Bridges, in the corrupting of the Silk Road investigation. However, there were

other revelations, in both kind and degree, that appeared for the first time in the Force Complaint, but which should have been disclosed to the defense herein earlier, and even before trial.

As discussed *ante*, the investigation of former SA Bridges was already fully underway by Fall 2014, and his misconduct, was known by then as well (as demonstrated by the contents of the interviews of him). Former SA Bridges's relevance to this case is beyond obvious: as the Force Complaint attests, former SA Bridges "had been assigned to the Secret Service's Electronic Crimes Task Force." Force Complaint, at 40. Also, former SA Bridges's "specialty was in computer forensics and anonymity software derived from TOR." *Id.* Former SA Bridges was also "the Task Force's subject matter expert in Bitcoin." *Id.*

Beyond his particular expertise, firmly in the wheelhouse of multiple critical aspects of this case (computer forensics, TOR, and Bitcoin), former SA Bridges placed himself firmly in the middle of important factual issues, such as his serving as the affiant for the seizure of Mark Karpeles's Dwolla accounts in May 2013. *Id.*, at 41. Former SA Bridges also, according to the Force Complaint, served as the affiant for other documents. *Id.*, at 41.

In addition, former SA Bridges clearly worked in concert with former SA Force. *Id.*, at 43, 45. Thus, former SA Force was assisted in his illegal, unauthorized infiltration and manipulation of the Silk Road website by a computer forensics with expertise in anonymity and Bitcoin. Yet none of this information was disclosed to the defense herein until the filing of the Force Complaint. Clearly, the government at some point and in some fashion abandoned its "abundance of caution" policy altogether.

The timing, volume, and sophistication of former SA Force's Bitcoin transactions were

also provided for the first time in the Complaint. *See* Force Complaint, at 4 (former SA Force “engaged in a series of complex transactions between various Bitcoin accounts . . .”). Former SA Force received “several large international and domestic wire and Automated Clearing House (ACH) transfers through the latter half of 2013 and first half of 2014.” *Id.*, at 7.

Former SA Force’s deposits totaled at least approximately \$757,000 “for the roughly year long period beginning April 2013 through May 2014.” *Id.*, at 7-8 (footnote omitted). Nor does that include other deposits made afterward. *Id.*, at 8 n. 2. Any deposits made in the first half of 2014 would of course have occurred *after* Mr. Ulbricht had been arrested, begging the question of the source of those funds.⁸

The Force Complaint also divulged former SA Force’s additional misconduct, which sheds light on his capacity for fraud, deception, forgery, abuse of his government authority and access – including predatory and retaliatory conduct and false accusations against innocent persons – and inventing complex, layered cover stories to conceal his misdeeds.

For example, the Force Complaint, at 29-33, in a section entitled “FORCE’s Unlawful Seizure of R.P.’s Funds,” details former SA Force’s series of attempts to convert the contents of an account held by “R.P.,” which efforts included abuse of various criminal law enforcement

⁸ Regarding the value of the Bitcoins former SA Force received via Silk Road, the Complaint notes how those quantities could be leveraged into extraordinary sums depending on when they were exchanged, *see* Force Complaint, at 15 & n. 8, (a concept the government resisted at trial but now embraces) with the maximum value reached soon after Mr. Ulbricht’s arrest, a time – perhaps not coincidentally, when former SA Force attempted to cash out. *See Id.* (“during the time FORCE was liquidating bitcoins through his own personal accounts, the value of bitcoin fluctuated dramatically ranging from less than \$300 per bitcoin to over \$1100 per bitcoin”). *See also id.*, at 43 n. 26 (at its peak value in Fall 2013, the 20,000 bitcoins delivered January 25, 2013, from Silk Road accounts to a bitcoin wallet address would have been worth “in excess of \$20 million”).

privileges and false accusations against “R.P.” to justify seizure of the account.

Former SA Force also misused subpoenas and in effect committed forgery by using his supervisor’s stamp. *See id.*, at 29, 33-34, 35. *See also id.*, at 4 (former SA Force “used his supervisor’s signature stamp, without authorization, on an official U.S. Department of Justice subpoena and sent the subpoena to a payments company, Venmo, directing the company to unfreeze his own personal account”). He also improperly performed queries in law enforcement criminal databases. *See Force Complaint*, at 27.

Moreover, former SA Force “‘papered up’ the seizure of the digital currency portion of” one of his victim’s accounts “in such a way that he may have thought he would be covered in the event anyone ever asked any questions” about his conduct.” At 32. *See also id.*, at 33 (former SA Force’s documentation was an “attempt to give himself plausible deniability by memorializing the digital currency seizure . . .”).

Thus, the extent and in some respects the nature of former SA Force’s misconduct – as well as former SA Bridges’s participation altogether – was hidden by the government from the defense in this case until well after trial.

E. *What Remains Unknown (to the Defense, At Least) About SA Force’s and Bridges’s Misconduct In the Context of the Silk Road Investigation*

Nor can the government state the extent of that misconduct, which raises additional questions about what remains unknown. In fact, the government – even in the Force Complaint, or in any other context – cannot confirm the full range of former SA’s Force and Bridges’s misconduct and illegal activities in connection with the Silk Road site and investigation. Nor can the government produce or confirm the full range of communications and/or relationship between former SA’s Force and Bridges with Dread Pirate Roberts, or any other person or entity

involved in the Silk Road site.

In fact, as the Force Complaint acknowledges with respect to the contacts between former SA Force and DPR, “[m]any but not all of their communications were encrypted[.]” *Id.*, at 12. Also, while “[s]ome portion of the communications between DPR and Nob (FORCE) are memorialized in FORCE’s official case file . . .” and “[s]ome of the communications are also preserved on FORCE’s official computers[.]” nevertheless “not all of the communications between DPR and Nob (FORCE) were memorialized.” *Id.*, at 12.

Nor did former SA Force memorialize in any government file or computer his private key necessary to decrypt those PGP-generated communications with DPR. As a result, as the Complaint notes, the government cannot even provide a full account of former SA Force’s communications with DPR. *Id.*, at 13-14. The Force Complaint also concluded that the encryption and failure to memorialize the private key was indicative of former SA Force’s intent to conceal those communications from the government and that the reason was because they were corrupt communications. *Id.*, at 13-14. *See also id.*, at 13 (“the communications should have been documented, in deciphered form, and memorialized in the file”).

The encrypted communications grew in frequency as the relationship between former SA Force and DPR progressed: “toward the end of the timeframe in which Nob (FORCE) was in relatively heavy communication with DPR, FORCE increasingly was not providing the decrypted versions of their communication.” *Id.*, at 14.

For instance, for the chain of messages between former SA Force and DPR from July 31, 2013, through August 4, 2013, all but one of the messages (which was from DPR) are completely encrypted. *Id.*, at 16. Also, the communications between French Maid (another of

former SA Force's aliases)⁹ and DPR, spanning from August 26, 2013, through September 13, 2013, were also predominantly encrypted. *See* Force Complaint, at 21. However, the Force Complaint tells only part of the encryption story, as review of discovery establishes that the range of Nob's encrypted communications with DPR was from January 29, 2013, through August 4, 2013.

As evidence of some of the encrypted communications between former SA Force and DPR, the Force Complaint also cites the portions included in the "LE_counterintel" file (proposed Defendant's Exhibit C at trial in this case) found on Mr. Ulbricht's laptop, which file, in response to government objections discussed in a sealed robing room conference prior to court February 3, 2015, the defense was permitted only to summarize – and only portions thereof (despite the defense's request to admit the entire document and/or read from additional sections). *See also* Force Complaint, at 20 ("the file appears to contain cut and pasted sections of what the insiders were relaying to [DPR] through online chats or private messages."

Yet the Complaint acknowledges the importance of that LE_counterintel file: "[p]rior to his arrest, DPR was known to have been hiding his true identity and location from law enforcement, so information concerning the government's investigation was material and valuable to him." *Id.*, at 13.

Also, the government cannot provide any assurance that *all* of former SA Force's communications with DPR – regardless of the particular alias utilized by former SA Force –

⁹ Interestingly, the Force Complaint cites as one basis for identifying former SA Force as French Maid their mutual use of an outdated version of software, the same technique used by SA Der-Yeghiayan with respect to Mr. Karpeles and the use of an outdated version of MediaWiki software. T. 659-63 (January 20, 2015).

have been preserved in *any* form, even encrypted. Nor is there any certainty with respect to how many aliases former SA Force employed – indeed, it was not until the defense pointed it out at trial that the government realized Death From Above was one of those aliases – or with whom he communicated with respect to Silk Road (via any system, *i.e.*, Silk Road Forum, private messaging, Tor chat, Pidgin chat).

Also unknown is the precise extent of former SA's Force and Bridges's compromising of the Silk Road website. In its Memo of Law, at 12 n. 3, the government provides bullet point arguments why what it describes as a defense "scenario was implausible . . ." Of course, no SDNY AUSA has ever described any defense as "plausible," but in any event that is an argument with respect to the *weight* of the evidence, an issue for the jury.

Nor are the government's arguments persuasive in any event. The codebase for the Silk Road site, PHP myadmin,¹⁰ provided in discovery reveals that an administrator with the level of access granted to the user "Flush" could have reset the PIN on DPR's account and usurped control of it. Indeed, at the December 15, 2014, pretrial conference (previously sealed portion), the government could not state for certain what level of access former SA Force possessed as a result of his corrupt activities. *See* Transcript, December 15, 2014, at 40-43.

With PHP myadmin access, Flush (whose account former SA Force initially hijacked), or anyone (such as former SA's Force and/or Bridges) could have changed anything in the Silk Road database, including message text in the Forum or Market messages, and re-set passwords. There were multiple PHP myadmin accounts; therefore, Flush (or someone acting as him) could have had access to DPR's account without DPR losing access.

¹⁰ PHP is a server-side scripting language and can be used to build web applications.

In addition, the second SSH key – to which government witness Brian Shaw testified to at trial, *see* T. 1970-71 (February 2, 2015), unquestionably provided root access to the Silk Road server(s), and it is unknown who had access via that SSH key, or when it was created. Mr. Shaw did testify, however, that the “Frosty” SSH key was modified March 26, 2013, certainly after former SA’s Force and Bridges’s corrupt access to the Silk Road site.

Also, in a TOR chat log commencing February 17, 2012, at 19:14, DPR and Inigo (another administrator for the Silk Road site), there is discussion for approximately half an hour regarding privileges provided to Inigo for access to the Silk Road *database*. It is unclear whether Flush was granted the same access, but certainly the government has not established that Flush did not enjoy such access. In addition, the government’s contention about the private key is meritless, as that key could easily have been duplicated.

Absent the opportunity to inspect items relevant to the investigation of former SA’s Force and Bridges, the full extent of potentially exculpatory material cannot be determined. At this point, the defense has only a limited idea of the extent to which former SA’s Force and Bridges were able to penetrate the Silk Road site given their level of administrative access. From information publicly available about the investigation, though, it appears that certainly former SA Bridges, and even former SA Force, had a relatively high level of technical sophistication. It is feasible that given their level of access, former SA’s Force and Bridges could have been able to exploit vulnerabilities in the site to gain access to other administrative accounts, or possibly even the Dread Pirate Roberts account.

In that context, if the defense theory was “implausible,” there was certainly no harm in its admission at trial. Rather, the government’s still feverish efforts to preclude presentation of that

evidence demonstrates that it was material to the trial. Moreover, the information regarding former SA's Force and Bridges cannot be viewed in isolation. Instead, it must be evaluated along with other evidence the defense introduced at trial, and which it offered but was denied admission. Taken together, that evidence provides a compelling defense that Mr. Ulbricht should have been allowed to present to the jury.

Another still unknown aspect is the contents of the still-sealed paragraph (at 11) in the Force Complaint. In addition, the Force Complaint itself notes that it "does not include certain additional facts known to me and the government's investigation continues." *Id.*, at 6.

F. *The Record Demonstrates That Silk Road Investigations Were Coordinated and, for Practical Purposes and for Determining Relevance to This Case, Combined*

The government's repeated insistence that the Southern District of New York's investigation was "independent" of that in which former SA's Force and Bridges were involved is demonstrably repudiated by the record *created by the government's investigators and prosecutors themselves*.

That record establishes that all of the federal investigations of the Silk Road website, were coordinated and, for practical purposes, combined. To the extent there is any question with respect to that conclusion, it is respectfully submitted that the Court should order and conduct an evidentiary hearing on the issue.

By any conception of "independence," these investigations do not qualify. Rather, they were decidedly *interdependent* because, as detailed below,

- the agents conducting the investigation were in continued contact with each other regarding the status of the investigations;
- supervisory law enforcement officials coordinated the investigations;

- each investigation made its fruits available to the other, and used that information from the companion investigation(s);
- information was entered in law enforcement databases to which all federal law enforcement enjoyed access;
- the investigations sought information about and from the same targets at the same time; and
- ultimately, SDNY was able to dictate the distribution of federal charges in the case for *all* of the districts involved in the coordinated investigations.

The 3500 material produced for SA Der-Yeghiayan serves as a catalogue of the interaction and linkage of the various investigations of the Silk Road website. For example, a report by SA Der-Yeghiayan regarding his investigation of Mr. Athavale (discussed in more depth *ante*, at 26-30), notes that in October 2012, “HSI Baltimore office provided SA Der-Yeghiayan with a file containing all of the Undercover (UC) chats made between a UC agent and DPR.” 3505-3072 (attached hereto as part of Exhibit 4).

Similarly, in a May 22, 2013, e-mail to Lisa M. Noel, an HSI intelligence analyst with HSI Baltimore (and part of that Silk Road Task Force), SA Der-Yeghiayan wrote that “[w]e would like to examine some of the language, usage, diction, etc. with the new U/C chats from Nob.” 3505-628. *See also* 3505-630 (in a November 2, 2012, e-mail regarding analyzing Mr. Karpeles’s writing, SA Der-Yeghiayan remarks that “[t]his professor knows dread’s writing better than anyone, it would be good to show him raw posts that are unedited”).

Thus, at the outset of his investigation – which the government cannot claim was “independent” of the case against Mr. Ulbricht – SA Der-Yeghiayan was provided with the

principal product of the Baltimore investigation, *generated by former SA Force himself*. Thus, the connection is inescapable, regardless of the government's mantra of "independence."

Other e-mails and reports authored by SA Der-Yeghiayan describe the continued contacts. In a May 15, 2013, e-mail, SA Der-Yeghiayan wrote that "[i]n early August 2012, HSI Chicago notified HSI Baltimore of the connection made [between Mr. Karpeles and Silk Road] and stated that Karpeles was a target of HSI Chicago's investigation." 3505-273. Also, "HSI Baltimore was provided a copy of the HSI Chicago's ROI [Report of Investigation] that highlighted all the facts of the connection." *Id.*

In that same e-mail, SA Der-Yeghiayan memorialized the following interaction:

HSI Chicago contacted HSI Baltimore and they confirmed that they shared all of HSI Chicago's information on KARPELES with members of their task force. HSI Chicago discovered that their IRS Agent, DEA Agent and SS Agent all inputted KARPELES into their individual investigations as a target and a potential administrator of the Silk Road based on HSI Chicago's ROI/information.

Id.

Subsequently, in an undated report, at 3505-273-75 (attached hereto as Exhibit 5), SA Der-Yeghiayan provided the following chronology:

- "[o]n May 10, 2013, [SA Der-Yeghiayan] was contacted by the HSI case agent and the Baltimore AUSA that the SS agent in their task force had issued a civil seizure warrant for Mutum Sigillum's Wells Fargo bank account. Both the case agent and AUSA stated they were not notified by the SS agent in their task force of the seizure warrant before it was already filed. The AUSA stated that he learned that the SS headquarters was notified that Wells Fargo had closed down

Mutum Sigillum account over suspicions of [18 U.S.C. §]1960 violations and the money was going to be returned to KARPELES. It is not exactly known at this time, but HSI Chicago believes that SS Headquarters notified the SS agent in Baltimore based on his record on KARPELES and therefore he got involved in making the seizure.” 3505-274;

- “[t]he following Monday May 13, 2013, HSI Baltimore and the Baltimore AUSA Justin Herring contacted HSA Chicago to notify him that they negotiated with SS Baltimore to seize the money in KARPELES’s Dwolla account using the same affidavit written by the SS. The total in the account was said to be over 3 million USD. HSI Baltimore stated that they would add Chicago’s project code for their CUC and case number to their seizure of 3 million.” 3505-275;
- “[t]he Chicago AUSA Marc Krickbaum is aware of both seizures and has informed the AUSA Justin Herring in Baltimore that Chicago was still intending on possibly pursuing criminal charges for 1960 violations that occurred in the State of Illinois. AUSA Marc Krickbaum had no objections to the SS seizure or HSI’s seizure over the accounts even though HSI Chicago felt they should be making the seizure on the Dwolla account.” *Id.*;
- “[i]t is HSI Chicago’s and HSI Baltimore’s case agent’s position that the SS Baltimore Agent would never have been alerted by SS headquarters about KARPELES’s bank account had it not been for the record they entered as a direct result of it being provided to them by HSI Chicago through HSI Baltimore. HSI Chicago is the source of the information for Baltimore’s work on KARPELES as

well. HSI Chicago maintains the longest standing TECS records on KARPELES, and exclusive TECS records on Mt. Gox and Mutum Sigillum.” *Id.*;

- “[c]ase agent Jared Der-Yeghiayan is also of the opinion that HSI Baltimore should have offered to defer the Dwolla seizure of 3 million USD plus to HSI Chicago knowing that they had developed the charges in their district and were pursuing criminal charges.” *Id.*

Another, (seven-page) report from SA Der-Yeghiayan regarding various investigations into Silk Road further recounts their interlocking character. 3505-295-301 (attached hereto as Exhibit 6). For example,

- January 13, 2012, a Baltimore HSI supervisor “requested a phone call about HSI Chicago’s Silk Road case.” 3505-295;
- February 1, 2012, representatives of HSI Baltimore flew to Chicago for a meeting regarding the Silk Road investigation. AUSA’s from both jurisdictions attended, as did HSI case agents and other personnel (including an Intelligence Analyst). *Id.*;
- during that February 1, 2012, meeting, HSI Baltimore “requested to split up our investigation so they could work a section of it[,]” to which HSI Chicago “strongly disagreed and stated that they were fully advance[d] in the case and did not see any advantage to give up any aspect of their investigation which included the administrators and organizers.” *Id.*;
- HSI Baltimore claimed to have an informant who would enable HSI Baltimore to “take down the site within a week or two with that information.” HSI Chicago

“disagreed that could be done and disagreed with the strategy they intended to take and stated they were working all aspects of the investigation and wanted to send a message with the case.” 3505-296;

- “[t]he [February 1, 2012] meeting ended with HSI Baltimore stating that they intended on shutting down the website soon and weren’t concerned with HSI Chicago’s strategy but they would coordinate once they take the website down.” *Id.*;
- communications between HSI Chicago and HSI Baltimore continued with respect to the status of the investigation of Silk Road. *Id.*;
- in April 2012, HSI Chicago developed a new informant and informed HSI Baltimore. According to SA Der-Yeghiayan’s report, “HSI Baltimore requested access directly to the informant but wouldn’t tell HSI Chicago why they wanted access or what they wanted to ask the CI [Confidential Informant]. HSI Chicago offered to take any questions and directly ask the CI the questions for them, but they would not allow access to the CI without knowing any topic of questions. HSI Baltimore expressed anger over not being allowed direct access to the CI.” *Id.*;
- in July 2012, HSI Chicago identified Mark Karpeles as a target of the investigation, and entered a record to that effect in the TECS system, to which all federal law enforcement agencies have access. 3505-296-97;
- July 9, 2012, a Baltimore HSI agent “wanted to send out a draft for HSI Headquarters notifying all HSI offices that he is the POC [point of contact] for all

Domestic Silk Road related investigations and that HSI Chicago will be the POC for all international related investigations. HSI rewrote HSI Baltimore's draft to state that they were [either redacted or missing]." 3505-297;

- during July 2012, more inquiries arose with respect to coordinating the HSI Chicago and HSI Baltimore investigations of the Silk Road website (*id.*);
- August 3, 2012, [HSI supervisory officials] informed SA Der-Yeghiayan that they believed HSI Baltimore wanted funding to travel to the foreign country to interview [Mr. Karpeles]." In response, SA Der-Yeghiayan sent an e-mail to HSI Baltimore agents "notifying them that [Mr. Karpeles] was more involved in the Silk Road and was a target o[f] their investigation, and asked in the email not to share the information with the rest of their unofficial Task Force." *Id.*;
- August 23, 2012, "HSI Chicago was called to a meeting at [HSI supervisory offices] to meet with HSI Baltimore and each present their cases to both SACs [Special Agent in Charge] Operations each of their cases. At the end of the presentations both HSI Baltimore and HSI Chicago's Operations Managers were discussing the confusion and odd approach to the HSI Baltimore's investigation and asked HSI Chicago if [HSI Baltimore's] investigative methods are interfering with HSI Chicago's case. HSI Chicago expressed deep concern for HSI Baltimore's tactics and the lack of focus in their investigation." *Id.*;
- in October 2012, an HSI Baltimore agent "began asking SA Der-Yeghiayan for all his information on [Mr. Karpeles] because they were trying to work him too. In response, SA Der-Yeghiayan "informed [the HSI Baltimore agent] to not work

[Mr. Karpeles] independent of HSI Chicago.” 3505-298;

- “HSI Chicago later discovered that HSI Baltimore had disseminated [Mr. Karpeles] to all members of their task force and they had issued multiple subpoenas on [Mr. Karpeles], and actively worked him to include a type of surveillance without the knowledge of HSI Chicago.” *Id.*;
- “[i]n early October 2012, HSI Chicago began developing a method to identify the main administrator of the website by analyzing thousands of pages of text on various websites to make a match. In early November 2012, HSI Baltimore offered to provide UC [Under Cover] Chat information with the administrator to help HSI Chicago with their development. HSI later identified a target [Anand Athavale] and began issuing subpoenas to further the identification and location of [Mr. Athavale]. HSI Chicago informed HSI Baltimore and shared the subpoena information with HSI Baltimore.” *Id.*;
- in December 2012, HSI Baltimore continued to request from HSI Chicago information regarding Mr. Karpeles. 3505-299. In late April 2013, “HSI Baltimore stated that they had looked heavily on their own into [Mr. Karpeles] and don’t believe [Mr. Karpeles] is involved in the website no longer. HSI shared a few of their subpoena returns they received in early May.” *Id.*;
- May 10, 2013, “[HSI] Baltimore notified HSI Chicago that the SS agent in their Task Force went ‘rogue’ and seized the bank account in the U.S. containing 2

million dollars from [Mr. Karpeles].¹¹ HSI Baltimore claimed to have no knowledge of the seizure until after it occurred. HSI Baltimore also admitted that they told the SS agent of the connections HSI Chicago made to the Silk Road back in August of 2012. HSI Baltimore stated that the SS agent went to a totally different AUSA in their District to file the affidavit to seize the account.” *Id.*,¹²

- May 13, 2013, “HSI Baltimore called HSI Chicago and stated that they had complained enough to the SS about the way the agent went behind their back that the SS agreed to give HSI the other account containing 3 million USD belonging to [Mr. Karpeles]. HSI Baltimore proceeded to ask HSI Chicago if they could provide any other bank accounts belonging to [Mr. Karpeles] so they could seize those accounts too. HSI Baltimore proceeded to seize the 3 million USD using the same affidavit written by the SS agent except [the HSI Baltimore agent] substituted his name and knowing that HSI Chicago built their pending charges [against Mr. Karpeles] on those seizures.” *Id.*,¹³

¹¹ As the Force Complaint states, May 9, 2013, former SA Bridges “served as the affiant on a multi-million dollar seizure warrant for Mt. Gox and its owner’s bank accounts” two days after receiving a large wire transfer from Mt. Gox and benefitting in the amount of \$820,000 from a Mt. Gox account. Force Complaint, at 5. *See also id.*, at 9, 45.

¹² Despite the concentration on this issue during cross-examination of SA Der-Yeghiayan, and the government’s related motion to preclude cross-examination and strike testimony, the government remained inexplicably mum regarding its knowledge of former SA Bridges’s role in securing that seizure affidavit. If there is any question regarding what the government knew and when it knew it, it is respectfully submitted that the Court should order and conduct an evidentiary hearing on the issue.

¹³ While HSI Chicago had expressed its intention to seek charges against Mr. Karpeles for violating 18 U.S.C. §1960 (operating an unlicensed money service business), HSI Baltimore had decided it would not pursue such charges. 3505-298.

- during a May 17, 2013, conference call that included as participants an AUSA from the Northern District of Illinois, two AUSA's from the District of Maryland, and HSI agents from both HSI Chicago and HSI Baltimore, one of the D.Md. AUSA's "stated they were trying to work on an interview with [Mr. Karpeles] with [Mr. Karpeles's] attorneys." The N.D. Illinois AUSA "asked what the purpose of the interviews was and [the D.Md. AUSA] stated they wanted to know more about [Mr. Karpeles's] money business and wanted to ask him directly about his knowledge of the Silk Road." In response, "HSI Chicago expressed serious concern over that approach and was concerned as to [the D.Md. AUSA's] using HSI Chicago's information developed on [Mr. Karpeles] for their own use." Ultimately, the "outcome of the" conference call was that one of the D.Md. [3505-299-300;
- HSI Chicago and HSI Baltimore conducted a "joint" search warrant "based on a new target developed by HSI Chicago." 3505-300;
- HSI Chicago and HSI Baltimore conducted another conference call July 9, 2013, about the Silk Road investigation. *Id.* During that call, neither the HSI Baltimore agents nor the D.Md. AUSA on the call mentioned – despite a question from SA Der-Yeghiayan whether there were any new developments – that another D.Md. AUSA had scheduled a meeting with Mr. Karpeles's attorneys. *Id.* That meeting occurred July 11, 2013. *Id.* During the meeting, Mr. Karpeles's attorney "randomly brought up the Silk Road and stated that their client was willing to tell them who [Mr. Karpeles] suspects is currently running the website in order to

relieve their client of any potential charges for [18 U.S.C. §1960].” *Id.* Also, the D.Md. AUSA “proceeds to set up a meeting with [Mr. Karpeles] overseas.” *Id.* HSI Chicago did not learn of the July 11, 2013, meeting with Mr. Karpeles’s attorneys until July 16, 2013. *Id.* Subsequently, one of the D.Md. AUSA’s informed SA Der-Yeghiayan that the other D.Md. AUSA “continued to negotiate with [Mr. Karpeles’s] attorneys” – despite SA Der-Yeghiayan’s objections – and has changed the meeting location to Guam [] later on in August. *Id.*;

- July 12, 2013, there was a “coordination meeting with HSI Chicago, HSI Baltimore, *FBI New York* and multiple DoJ [Department of Justice] attorneys and CCSIP attorneys[.]” 3505-300. At that “coordination meeting, “HSI Chicago mentioned [Mr. Karpeles] as their main target.” *Id.*;

A month later, in August 2013, SA Der-Yeghiayan swore to the affidavit, composed by AUSA Turner, in support of the SDNY search warrant application for Mr. Karpeles’s e-mail accounts. Again, in light of this overwhelming evidence, any claim of “independence” is untenable. In the event there remains any question, it is respectfully submitted that an evidentiary hearing is necessary to challenge the government’s utterly unreliable and unsupported assertions (that are contradicted by the government’s own documents).¹⁴

Nor was former SA Force’s investigation into Silk Road was transitory or superficial in any respect. It began in February 2012, *see* Force Complaint, at 22 n.14, and generated dozens of DEA-6 reports of his (authorized) undercover activities investigating the Silk Road website.

¹⁴ A separate question that merits an answer is whether any evidence related to Nob or Flush was introduced in the grand jury that indicted Mr. Ulbricht.

In fact, as the Force Complaint points out, information-sharing, and its impact relevant to this case, continued through the summer of 2013: “by late July 2013, the Baltimore Silk Road Task Force had been made aware that the FBI was seeking to obtain an image of the Silk Road server, and therefore FORCE may have had reason to fear that any communications between himself and DPR would be accessible to the FBI in the event the FBI was successful in imaging the server.” Force Complaint, at 17-18.¹⁵

Even the government’s Memo of Law, at 14 n. 4, contradicts its naked claim of “independence.” That footnote, in explaining the government’s realization (after the defense attempted to introduce certain documents provided in discovery) that DeathFromAbove was among former SA Force’s aliases, states that “former SA Force had access to law enforcement reports filed by SA Der-Yeghiayan, including reports concerning his suspicions regarding Anand Athavale, which was likely the source of the information leaked by Force through the “DeathFromAbove” account.” (Citation omitted).

Ultimately, the investigations were not only interrelated and interdependent, but their outcomes were dictated by SDNY. As SA Der-Yeghiayan reported in a September 20, 2013, e-mail to an HSI colleague,

¹⁵ That would also ostensibly have provided DPR, via former SA Force as Nob (or French Maid, or alpacino, or DeathFromAbove, or perhaps some other incarnation) with advance notice of the FBI’s imaging of Silk Road’s servers – consistent with the defense’s position that DPR purchased and/or was provided with information that permitted him to formulate and implement – with former SA Force’s (and perhaps former SA Bridges’s) assistance – an escape plan that also incriminated Mr. Ulbricht falsely. In that context, former SA Force also learned at least days in advance that law enforcement intended to make an arrest of DPR in late September 2013, thereby giving him ample time to warn DPR. *See* Force Complaint, at 18 & n. 10. Yet Mr. Ulbricht did not assume any additional security protocols, but instead violated even the most fundamental security precepts in multiple ways.

I think that would be a good pitch but that they can't expect to take an admin or something – they all need to be prosecuted out of the same AUSA's office under a conspiracy – NY will never agree to anything else. It's not like they can give them an admin, that makes no sense from a prosecutorial standpoint.

Baltimore can have a few vendors of our choosing – as well as the ability to say they “helped” ID some of the admins by “allowing” NY to use OUR UC account to identify some of the lower admins, and they can have sloppy seconds on DPR for their murder for hire. They can also have some info on other bitcoin companies that MK might name is shady after we get done with him.

That's the best that can be given and they should consider themselves lucky for getting anything close to that. Or we can just stall, and Baltimore gets nothing and we contributed to the other two admins getting away [redacted]. We'll get no HSI banner on the site, and will probably get no cooperation from NY with any information related to MK. If DPR names MK in the interview and we didn't help them get the other admins when we had the chance – NY will leave us out of it and tie him into their conspiracy. We will then be left dealing with HSI Baltimore's tears and them then trying to take [redacted].

I think it's important we help them have a “come to Jesus” moment otherwise our agency loses as a whole. It's a simple sell if they know the alternative is they will be left with absolutely nothing – no matter how much they whine and complain to HSI HQ, it won't stop the SDNY from prosecuting all of them without any of us.

3505-319 (attached hereto as Exhibit 7).

A half-hour later that same day, September 20, 2013, SA Der-Yeghiayan e-mailed that same colleague with the following message:

I think there's room to avoid the drama by instead of dwelling on the past or trying fluff up each others cases under the false assumption that the website will be up in the next month to talking about how to try and make HSI in general walk away from this without looking like complete fools. But it has to start with HSI Baltimore conceding that they will not be identifying or prosecuting dread first or any other admin for a fact. Then realizing that they still stand a chance, if they play nice, to walk away from this with something to show from their “investigation.”

They can easily erase a lot of the damage they've done by cooperating with NY's almost guaranteed prosecution of the website.

The only two options are remain in denial and walk away with nothing but blame and egg on their face in the next few weeks, OR play nice and possibly take some credit for the identification and prosecution of all the admins, and reap some of the benefits by prosecuting some of the vendors our defendant is going to identify. No other way forward than that.

3505-320 (attached hereto as Exhibit 7).

Thus, in light of all of the evidence set forth above, the interdependence and continuing relationship among the investigations, including that in which former SA's Force and Bridges participated, is indisputable.

G. *The Information Regarding the Investigation of Former SA's Force and Bridges Would Be Relevant to This Case Regardless Whether the Investigations Were Independent*

Even assuming *arguendo* the SDNY investigation was "independent" from the District of Maryland investigation, the information and material regarding former SA's Force and Bridges was, *as evidenced by the government's own strategy in preparing for trial herein*, as well as other objective indicia, plainly relevant to this case.

1. *The Government's Initial Exhibit List*

The government's initial Exhibit List was provided December 3, 2014 – two days *after* the government's November 21, 2014, letter to the Court setting forth information regarding the investigation of former SA Force was disclosed to the defense – included a number of documents and materials directly relevant to former SA Force. For example,

- GX 220 was a Torchat buddy list that contained the identification for “Nob,” an account operated by former SA Force;
- GX 225 was a Torchat between DPR and “Scout,” dated January 26, 2013, in which DPR stated, “I’m not even going to hurt this guy that ripped me off if I can help it. This isn’t the mob or cartel.” Given the time frame of the chat, that is most likely a reference to “Flush,” an account ultimately operated by former SA Force, and the administrator who was the subject of the alleged murder-for-hire scheme in which Nob was involved;
- GX 227 was a Torchat log between DPR and Cimon dated January 26, 2013, in which DPR stated, “had a csr go rogue and rip me off for 350k.” That, too, related to the “Flush” account that ultimately was under former SA Force’s control, and which he allegedly used to steal funds from the Silk Road website. The discussion also references Nob’s involvement in the first alleged murder for hire plot;
- GX 229A was a Torchat log containing a conversation dated January 26, 2013, between DPR and PatHenry, in which, at 6, DPR stated “also I have Flush (our new guy) ready for you.” That portion of the chat, however, was deleted from the exhibit ultimately entered into evidence at trial by the government as GX 229A;
- GX 229B was a Torchat log between DPR and Inigo containing multiple discussions regarding the “Flush” account, “Flush’s” whereabouts, the money “Flush” had allegedly stolen from the Silk Road site, and as to his capture;
- GX 241 was the unredacted journal for part of 2013 recovered from Mr.

Ulbricht's laptop. The journal includes mid-September 2013, entries regarding DPR's communications with Silk Road user "French Maid," and April 2013 entries regarding DPR's communications with DeathFromAbove. Also, log entries for June 5, 2013, to September 11, 2013, made reference to "alpacino," another one of former SA's Force's unauthorized user accounts, who had been "leaking info to [DPR;]"

- GX 243 was the "LE_counterintel" file in its unredacted entirety. It included multiple entries regarding information provided by alpacino and by another source, "East India Traitor" (whose identity has been determined, at least by the defense, but who could be former SA Force as well). A copy of that proposed Government Exhibit, which was offered by the defense at trial as Defendant's Exhibit C, is attached hereto as Exhibit 8;
- GX 250 was a computer file entitled "SR_accounting," an alleged Silk Road expense report, that included references to "theft from mtgox" as well as regular payments to hackers and other extortionists, a large number of which occurred in the spring and summer of 2013;
- GX 252 was a document titled "todo_weekly.txt" which contained a section entitled "pay employees" that listed "albertpacino" as receiving \$500 per week;
- GX 275 was a document entitled "ops.txt," and which was ultimately redacted to remove references to Curtis Green and his bitcoin address, both of which were related to the first alleged murder for hire plot involving former SA Force) by the government prior to its admission into evidence.

2. *The Government's Opposition to Mr. Ulbricht's Motion for Bail*

The government also relied on former SA Force's work in opposing Mr. Ulbricht's application for bail in November 2013. The government's November 20, 2013, letter included the following passages:

- “[t]he Complaint also describes how Ulbricht was willing to use violence to protect his online drug empire, commissioning multiple murders for hire in seeking to guard his interests in Silk Road. Ulbricht has been separately charged for one of these attempted murders for hire in an indictment issued by the United States Attorney’s Office for the District of Maryland, unsealed on October 2, 2013.” Gov’t Letter, at 2. The government also attached the District of Maryland Indictment to its Response, as Exhibit B;
- “[m]oreover, he repeatedly resorted to violence in seeking to protect his lucrative business, commissioning at least six murders for hire in connection with operating the site.” *Id.*, at 4;
- describing “no fewer than six murders for hire within a span of four months in 2013” that Mr. Ulbricht allegedly “commissioned,” followed by a detailed account of the chats between DPR and Nob and others, and payment particulars. *Id.*, at 5; and
- describing another chat between Nob and DPR regarding DPR’s concealment of his identity even from his girlfriend. *Id.*, at 10.

3. *The Importance of the First Half of 2013 Regarding the Evidence At Trial*

The relevance of the misconduct committed by former SA's Force and Bridges is also apparent from the time frame in which it is believed to have commenced and occurred – the first half of 2013. That period was critical in the context of the creation and collection of evidence used against Mr. Ulbricht at trial, and the defense's response to it.

A partial time line of relevant events during that span – described only by information possessed by the defense at the time of trial (and not including reference to former SA's Force or Bridges misconduct) – consists of the following:

- January 26, 2013: \$350,000 is taken from Silk Road accounts;
- January 26, 2013: DPR learns "Flush" has been arrested for cocaine possession;
- January 26-29, 2013: DPR discusses a murder for hire plot with several Silk Road administrators, as well as with a federal law enforcement agent posing as a Silk Road user;
- February 2013: "Nob" murder for hire plot against Flush allegedly occurs;
- March 13, 2013: discussion thread regarding "friendlychemist" and "redandwhite" begins (GX 936);
- March 16, 2013: User with user name "Ross Ulbricht" posts a question on Stack Overflow (T. 1343-44 [January 28, 2015]);
- March 16, 2013: publicly displayed user name on Stack Overflow account changes from "Ross Ulbricht" to "frosty" (GX 1200; T. 1343-46[January 28, 2015]);
- March 21, 2013,
March 25, 2013,
and April 11, 2013: Silk Road servers are subject to a DDOS (distributed denial of service) attack (T. 928 [January 21, 2015]; T. 1443 [January 28, 2015]; T. 1755 [January 29, 2015]; *see also* GX 241));

- March 26, 2013: SSH root access key to Silk Road servers modified to “frosty@frosty” (GX 901; T. 1753-1755 [January 29, 2015];
- March 31, 2013,
April 8, 2013,
and April 12, 2013: notable Bitcoin transactions occur those dates, as pointed out by SA Der-Yeghiayan in a September 16, 2013, e-mail (3505-355);
- April 1, 2013: communications to DPR from DeathFromAbove threatening DPR but also offering confidential law enforcement investigative information – including the name Anand Athavale as a government target – in exchange for payment begin (DX E);
- April 4, 2013: Email account associated with Stack Overflow account is changed from “rossulbricht@gmail.com” to “frosty@frosty.com” (T. 1347-48 [January 28, 2015]);
- April 15, 2013: murder for hire plot against “friendlychemist” allegedly carried out by “redandwhite” allegedly occurs, ending with a \$500,000 payment (GX 936);
- May 10, 2013: HSI Baltimore seizes more than \$2 million from accounts Mark Karpeles’s company holds at Dwolla, thereby notifying Mr. Karpeles that he is on the government’s radar (T. 729 [January 20, 2015]);
- Early June 2013: according to FBI Special Agent Christopher Tarbell, FBI first learns of the genuine IP address for the Silk Road servers (in Iceland) (*see* Declaration of former Special Agent Christopher Tarbell, at 3-4);¹⁶
- June 6, 2013: at the request of the U.S. government, law enforcement officials in Iceland image the Silk Road servers located there;

¹⁶ The government, however, had a lead on a different Silk Road server months prior: “[s]everal months earlier, the FBI had developed a lead on a different server at the same Data Center in Iceland (“Server-1”), which resulted in an official request for similar assistance with respect to that server on February 28, 2013.” *See* Tarbell Declaration, at 5 n.7.

- June 11, 2013: SA Der-Yeghiayan sends an e-mail noting the difficulty of determining the identities of users on the Silk Road site because multiple people were operating multiple accounts with different user names, leading him to ask, “Sheesh. Who’s on first?” (3505-03523-03524; T. 426-28 [January 15, 2015]; T. 633-34 [January 20, 2015]);
- June 2013: “alpacino” begins providing DPR confidential law enforcement information in return for payment (DX D [which is the same as initial GX 241]);
- July 2013: DPR assumes control of the Cirrus/ Scout account to obtain information about Mr. Wonderful, allegedly a federal law enforcement agent who had been investigating DPR;
- July 11, 2013: HSI Baltimore agents meet with Mr. Karpeles’s lawyers, who offer to reveal DPR’s identity in exchange for the government not bringing any charges against Mr. Karpeles (3505-300; T. 490-556 [January 15, 2015]);¹⁷ and
- July 23, 2013: FBI images the Silk Road servers located in Iceland.

4. *The Communications Between DeathFromAbove and DPR*

In foreclosing the defense’s use of any information or materials relating to former SA Force and his misconduct, the government exceeded the boundaries set by the Court in its pretrial rulings on the issue. While the embargo was supposed to cover only the information and materials generated as part of the ongoing grand jury investigation of former SA Force, at trial in this case the government converted that into a ban on the defense’s use of information and documents provided as part of discovery, which the defense had been expressly permitted to utilize at trial.

¹⁷ The 3500 material discussed *ante*, at 25, relating how Mr. Karpeles’s lawyers passed information about Mr. Ulbricht to the government, *see* 3505-2925, further connects the various investigations. Similarly, the interaction among investigations, and relevance to this case, is further established by the common mention of Mr. Athavale.

In fact, during the previously sealed portion of the December 15, 2014, pretrial conference, AUSA Turner, when asked by the Court about the parameters of the prohibition imposed on the defense by Rule 6(e), Fed.R.Crim.P., answered, “What they can’t reveal is that [former SA Force] is under a grand jury investigation. . . . It’s just a matter that he’s being investigated for [certain activities].” Transcript, December 15, 2014, at 48.

AUSA Turner added that

[s]o in terms of what [Rule] 6(e) prohibits, we think it prohibits them eliciting somehow that he’s under a grand jury investigation. That’s the basic point. I mean, that’s what 6(e) requires be kept secret while the investigation is pending. They still have many facts in their possession. They’ve had them in their possession long ago.

*Id.*¹⁸

Yet the communications between DeathFromAbove and DPR were *not* mentioned in the government’s November 21, 2014, letter to the Court, did not mention former SA Force at all, and did not disclose that he was under a grand jury investigation. Also, the government’s reaction at trial to the defense’s efforts to introduce those communications (as Defense Exhibit E, a copy of which is attached hereto as Exhibit 9), memorialized in the government’s

¹⁸ During the previously sealed portion of the December 15, 2014, pretrial conference, the Court recognized the government’s inconsistent and expansive position with respect to the scope of the Rule 6(e) proscription. In response to AUSA Turner’s remark that the “point is, we’re not trying to say certain witnesses, certain evidence is off limits. It’s the fact that this is a grand jury investigation. That’s what they’re prohibited from disclosing[.]” the Court replied

[w]ell, I hear what you’re saying. And it’s like ships passing in the night. *Because on the one hand it’s the content of the investigation.* And what you’re suggesting is it’s really not the content, it’s the fact of.

Transcript, December 15, 2014, at 49-50 (emphasis added).

(previously sealed) February 1, 2015, letter to the Court, makes it clear that the government had not made the connection between former SA Force and DeathFromAbove until the defense sought to introduce DX E. *See also* Government's Memo of Law, at 24 n. 10.

Nevertheless, at trial the government used the grand jury investigation of former SA Force as a sword to preclude far more than the mere fact that former SA Force was under investigation, and instead employed that excuse to eviscerate the defense and its attempts to introduce evidence not covered by the Court's pretrial rulings. In addition to the DeathFromAbove, the contents of Defense Exhibit E did not reveal that former SA Force was the subject of an ongoing grand jury investigation, yet the bulk of the information therein, as well as the document itself was precluded even though, as discussed **ante**, at 4, *it was included as a Government Exhibit in the initial list provided two days after the government disclosed to the defense the grand jury investigation of former SA Force.*

The government's account, in its Memo of Law, at 13-14, of its objections to the defense's attempt to introduce the private messages from "Death From Above" demonstrates the government's true objectives in precluding the information and evidence regarding former SA's Force and Bridges, which was simply to deprive Mr. Ulbricht of a defense at trial.

Conclusion

Accordingly, for all the reasons set forth above, and in Mr. Ulbricht's prior submissions, it is respectfully submitted that his motion for a new trial, pursuant to Rule 33, Fed.R.Crim.P., should be granted, and/or that his motion to suppress evidence be reopened and granted in its entirety.

Dated: 16 April 2015
New York, New York

Respectfully submitted,

/S/ Joshua L. Dratel
JOSHUA L. DRATEL
JOSHUA L. DRATEL, P.C.
29 Broadway, Suite 1412
New York, New York 10006
(212) 732-0707

Joshua J. Horowitz
225 Broadway, Suite 1804
New York, New York 10007
(845) 667-4451

Attorneys for Defendant Ross Ulbricht

– Of Counsel –

Joshua L. Dratel
Lindsay A. Lewis
Whitney G. Schlimbach
Joshua J. Horowitz